REMARKS

Initially, in the Office Action dated November 13, 2004, the Examiner rejects claims 3 and 13 under 35 U.S.C. §112, second paragraph. Claims 1, 4, 14 and 11 have been rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,825,891 (Levesque et al.). Claims 2, 3, 5-7, 12, 13 and 15-17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of U.S. Patent No. 5,958,053 (Denker). Claims 9, 10, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of Atkinson et al. RFC 2401.

By the present response, Applicants have amended claims 1-3 and 11-13 to further clarify the invention. Claims 1-20 remain pending in the present application.

35 U.S.C. §112 Rejections

Claims 3 and 13 have been rejected under 35 U.S.C. §112, second paragraph. Applicants have amended the claims of the present application to further clarify the invention and respectfully request that these rejections be withdrawn.

35 U.S.C. §102 Rejections

Claims 1, 4, 14 and 11 have been rejected under 35 U.S.C. §102(b) as being anticipated by Levesque et al. Applicants respectfully traverse these rejections.

Levesque et al. discloses enabling computers to communicate using encrypted network packets. A configuration request is sent over a network from a first computer to a second computer, and tunnel record information is sent over the network from the second computer to the first computer. The tunnel record

information is encrypted in accordance with a temporary configuration password. Updating a tunnel record is also disclosed where a connection request is sent from a first computer to a second computer and the first computer is authorized, a tunnel record corresponding to the connection request with the first computer's network address then being updated.

Regarding claims 1 and 11, Applicants submit that Levesque et al. does not disclose or suggest the limitations in the combination of each of these claims of, inter alia, prior to performing encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of the packet in a field in a header of the packet where the field is not subject to the encrypting security processing, the selected information including transport level information, the transport level information being usable by intermediate nodes between said node and said another node in the packet switched network to provide value added services relative to the transmission. In the §103 claim rejections section of the Office Action, the Examiner admits that Levesque et al. does not disclose or suggest selected information including transport level information, as recited in the claims of the present application, but asserts that Denker discloses these limitations at col. 3, lines 25-59. Since Denker was not used as a part of this rejection, this current §102 rejection has been successfully traversed since the Examiner admits that Levesque et al. does not disclose or suggest these limitations. However, Applicants will address the Denker reference here.

Denker discloses the TCP2B protocol and TCP2E protocol. In the TCP2B protocol, both client and server indicate their support for this protocol using one or more bits in TCP header. According to the TCP2B protocol, the client retransmits its requested options in the ACK message so the server need not store the options after the connection request. In the TCP2E protocol, the server maintains a Friends Table listing addresses of device recently observed to be complying with TCP. If a client's address is on the Friends Table, the connection request is processed according to TCP. Otherwise, the server sends an ACK message to the client to prompt the client to send a reset message. The client's address can then be added to the Friends Table.

The portions of Denker (col. 3, lines 25-59, cited by the Examiner as disclosing the limitations in the claims of the present application), merely discloses the Syncookie method as disclosed in Fig. 2. In this method, a server's Initial Sequence Number is generated by the server as a cryptologic function based upon the client's Initial Sequence Number, the client's IP address, and a secret known only to the server. After receiving a message from the client, the server can immediately check if the incoming acknowledgement number matches the appropriate hash function output and, if so, then the acknowledgement must have come in reply to a send ACK message from the server and the server can therefore trust the client. This is not, prior to encrypting security processing on a payload of a packet, storing information corresponding to selected information normally included in a payload of the packet in a field in a header of the packet where the field is not subject to

encrypting security processing, the selected information including transport level information usable by intermediate nodes between a sending node and a receiving node to provide value added services relative to the transmission, as recited in the claims of the present application. These portions of Denker do not disclose or suggest anything related to selected information normally included in a payload of a packet, or the selected information being transport level information usable by intermediate nodes to provide value added services. These portions of Denker merely disclose details of the commonly known Syncookie method. Denker discloses checking an acknowledgement message, not a header, as recited in the claims of the present application. Moreover, the Examiner fails to provide adequate motivation for one of ordinary skill in the art to combine Levesque et al. and Denker in that the only motivation provided is a description of the problem that Denker seeks to solve.

Regarding claims 4 and 14, Applicants submit that these claims are dependent on one of independent claims 1 and 11 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Applicants submit that neither Levesque et al. nor Denker disclose or suggest the selected information being stored in a security protocol header of the header of the packet, the security protocol header not being subject to the encrypting security processing.

Accordingly, Applicants submit that Levesque et al. (nor Denker) does not disclose or suggest the limitations in the combination of each of claims 1, 4, 14 and

11 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

35 U.S.C. §103 Rejections

Claims 2, 3, 5-7, 12, 13 and 15-17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of Denker. Applicants submit that these claims are dependent on one of independent claims 1 and 11 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. For example, Applicants submit that none of the cited references disclose or suggest value added services including differentiated services policing or metering, or transport level information including transport protocol information including TCP, UDP, ICMP, or port number information.

Accordingly, Applicants submit that neither Levesque et al. nor Denker, taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 2, 3, 5-7, 12, 13 and 15-17 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

Claims 9, 10, 19 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Levesque et al. in view of Atkinson et al. Applicants respectfully traverse these rejections.

Atkinson et al. discloses a document related to security architecture for the Internet protocol that specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP

layer, in both the IPv4 and IPv6 environments. The goals of such systems, their components and how they fit together with each other and into the IP environment is disclosed. The security services offered by the IPsec protocols, and how the services can be employed in the IP environment, are also described.

Applicants submit that claims 9, 10, 19 and 20 are dependent on one of independent claims 1 and 11 and, therefore, are patentable at least for the same reasons noted regarding these independent claims. Applicants submit that Atkinson et al. does not overcome the substantial defects noted previously regarding Levesque et al. For example, Applicants submit that none of the cited references disclose or suggest the encrypting security processing being performed according to the encapsulating security payload (ESP) or according to the authentication header (AH) protocol.

Accordingly, Applicants submit that neither Levesque et al. nor Atkinson et al., taken alone or in any proper combination, disclose, suggest or render obvious the limitations in the combination of each of claims 9, 10, 19 and 20 of the present application. Applicants respectfully request that these rejections be withdrawn and that these claims be allowed.

In view of the foregoing amendments and remarks, Applicants submit that claims 1-20 are now in condition for allowance. Accordingly, early allowance of such claims is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No. 01-2135 (referencing attorney docket no. 0173.37334X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP

Frederick D. Bailey
Registration No. 42,282

FDB/sdb
(703) 312-6600